Control Message)을 생성하여 출력하는 EMM/ECM 생성부(3), 상기 EMM/ECM 생성부(3)에서 입력된 제어 단어들 이용하여 방송 프로그램을 스크램블링하고, EMM/ECM 정보와 함께 다중화한 후, 전송 매체로 출력 송신하는 송신부(4)를 구비한 송신 장치; 및, 전송 매체를 통해 수신된 데이터를 역다중화하여 출력하는 역다중화부(5), 자신이 수신할 데이터이면 상기 역다중화부(5)에 제어 신호를 출력하여 역다중화한 후, EMM/ECM 정보를 출력하고, 제어 단어(CW)를 이용하여 수신한 스크램블링된 데이터를 복호화하는 디스크램블링하는 프로세서(6), 상기 프로세서(6)에서 입력된 EMM에서는 개인키를 복호화하고, 다시 이 복호키를 이용하여 더 세분화된 제어 단어(CW)를 ECM에서 추출하여 상기 프로세서(6)로 출력하는 스마트 카드(?)를 구비한 조건부 제한수신 서비스 시스템에 적용되는 메시지 처리 방법에 있어서, 최종 권한 키(OEK), 그룹 키(GK), 국번 권한 키(NEK)를 생성하는 제1단계(100 내지 103); 상기 제1단계(100 내지 103)에서 생성된 개인 키(PK)와 최종 권한 키(OEK)를 생성하는 제1단계(100 내지 103); 상기 제1단계(100 내지 103)에서 생성된 개인 키(PK)와 그룹 키(GK)를 이용하여 마스타 개인키(MPK)를 암호화하여 키값 변경을 위한 EMM 메시지 생성 후, 수신측으로 송신하는 제2단계(104, 105); 상기 제1단계(100 내지 103)에서 생성된 최종 권한키(OEK)를 개인 키(PK)와 그룹 키(GK)를 이용하여 암호화하고, 권한 부여 EMM 메시지를 생성한 후, 수신측으로 송신하는 제3단계(106, 107); 및 제어 단어(CW)를 생성한 후, 적절 권한 키(OEK)를 이용하여 제어 단어(CW)를 암호화하여 자격 제어 메시지(ECM)를 생성하고, 제어단어(CW)를 이용하여 방송 프로그램을 스크램블링한 후 수신에 송신하는 제4단계(106 내지 111); 및 포함하는 송신 과정과, 스마트 카드로부터 제공받은 마스타 개인키(MPK)를 이용하여 수신한 키값 변경을 위한 EMM 메시지를 복호화하여 복호화된 데이타를 암호화 이전의 체크섬(CSUM)이 유효한지 판단하는 제5단계(200 내지 202); 상기 제5단계(200 내지 202)에서 유효하면 개인 키(PK), 그룹 키(GK)를 획득하고, 수신한 암호 메시지를 획득한 개인 키(PK), 그룹 키(GK)로 복호화하여 복호한 데이터의 CSUM이 유효한지 판단하는 제6단계(203 내지 205) ; 및 상기 제6단계(203 내지 205)에서 유효하면 최종 권한키(OEK)를 획득하고, 획득한 최종 권한 키(OEK)를 이용하여 수신한 EMM 메시지를 복호화하여 제어 단어(CW)를 획득하고, 상기 제어 단어(CW)를 이용하여 방송 프로그램을 디스크램블링하여 출력하는 제7단계(206 내지 208); 를 포함하는 수신 과정으로 이루어지는 것을 특징으로 하는 조건부 제한수신 서비스를 위한 메시지 처리 방법.

청구항 2

제1항에 있어서, 상기 제1단계(100 내지 103)의 키 생성과정에 입력되는 데이타는, 확장 키 인덱스 값으로부터 64비트로 구성된 확장 키와 서비스 키인덱스 값으로부터 64비트로 구성된 서비스 키로 이루어지는 것을 특징으로 하는 조건부 제한수신 서비스를 위한 메시지 처리 방법.

청구항 3

제1항에 있어서, 권한 부여를 위한 EMM 메시지의 구조는, 메시지의 순서 번호를 나타내는 필드(Sequence), 다른 메시지의 존재 유무를 나타내는 필드(Append), 암호화시 홀수 또는 짝수 키를 사용 상태를 나타내는 필드(Encrypt)로 구성된 제어필드(CTRL)와, 벡터 갯수를 나타내는 필드(N)와, 벡터의 암호화에 사용된 키 번호를 나타내는 필드(KID)와, 채널 번호(ID), 홀수 서비스 키 주소(OSK), 짝수 서비스 키 주소(ESK), 홀수 확장 키 주소(ODK), 짝수 확장 키 주소(EDK), 자격 만료 기간을 표시하고, 카 생성 메트릭스 번호를 나타내는 Expiry/KM, 암호화 이전의 체크섬(checksum)을 나타내는 CSUM으로 구성된 다수의 암호화된 벡터 필드(Vector)로 구성된 것을 특징으로 하는 조건부 제한수신 서비스를 위한 메시지 처리 방법.

청구항 4

제1항에 있어서, 상기 키값 변경을 위한 EMM의 메시지의 구조는, 메시지의 순서 번호를 나타내는 필드(Sequence), 다른 메시지의 존재 유무를 나타내는 필드(Append), 암호화시 홀수 또는 짝수 키를 사용 상태를 나타내는 필드(Encrypt)로 구성된 제어 필드(CTRL)와, 벡터 갯수를 나타내는 필드(N)와, 벡터의 암호화에 사용된 키 번호를 나타내는 필드(KID)와, 변경할 키 번호를 나타내는 KID, 그룹 키일 경우 그룹 주소를 나타내는 BADDR, 홀수 서비스 키 주소(OSK), 짝수 서비스 키주소(ESK), 홀수 확장 키 주소(ODK), 짝수 확장 키 주소(EDK), 암호화 이전의 체크섬(checksum)을 나타내는 CSUM으로 구성된 다수의 암호화된 벡터 필드(Vector)로 구성된 것을 특징으로 하는 조건부 제한수신 서비스를 위한 메시지 처리 방법.

청구항 5

제1항에 있어서, 상기 자격 제어 메시지(ECM)의 구조는, 메시지의 순서 번호를 나타내는 필드(Sequence), 다른 메시지의 존재 유무를 나타내는 필드(Append), 암호화시 홀수 또는 짝수 키를 사용 상태를 나타내는 필드(Encrypt)로 구성된 제어 필드(CTRL)와, 벡터 갯수를 나타내는 필드(N)와 다수의 벡터 필드(Vector)로 구성된 것을 특징으로 하는 조건부 제한수신 서비스를 위한 메시지 처리 방법.

청구항 6

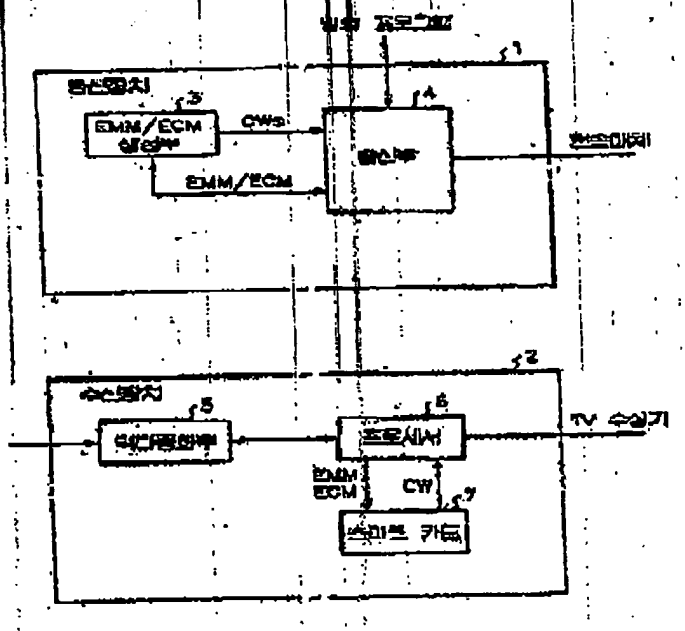
제5항에 있어서, 상기 벡터 필드(Vector)는, 채널번호(CH_ID), 채널 제어 필드(Chctrl), 홀수 제어 단어(OCW), 짝수 제어 단어(ECW), EPOCH 시간의 초단위 시간(time)과 채널의 형태(access), 현재 시스템 시간(month), 그리고, 암호화 이전의 체크섬(checksum) (csum)을 포함하는 필드로 구성된 것을 특징으로 하는 조건부 제한수신 서비스를 위한 메시지 처리 방법.

청구항 7

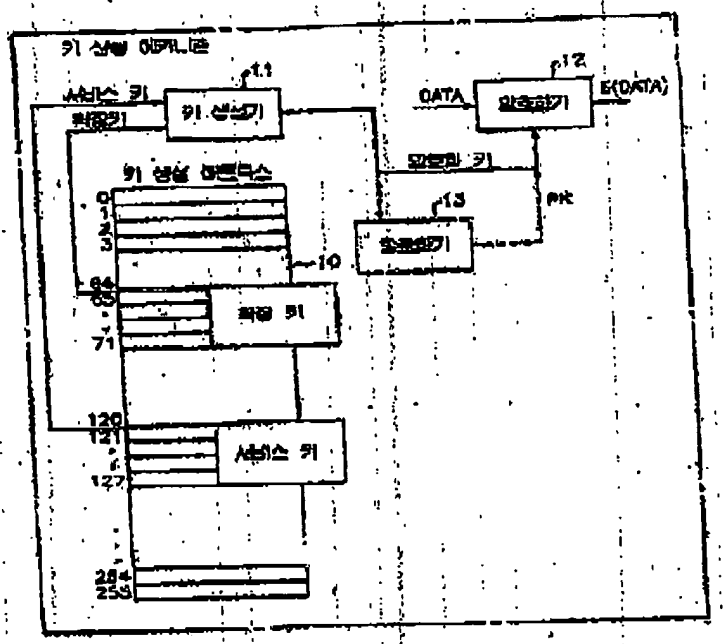
상기 OCW, ECW, time/access/month/csum은 암호화된 정보인 것을 특징으로 하는 조건부 제한수신 서비스를 위한 메시지 처리 방법.

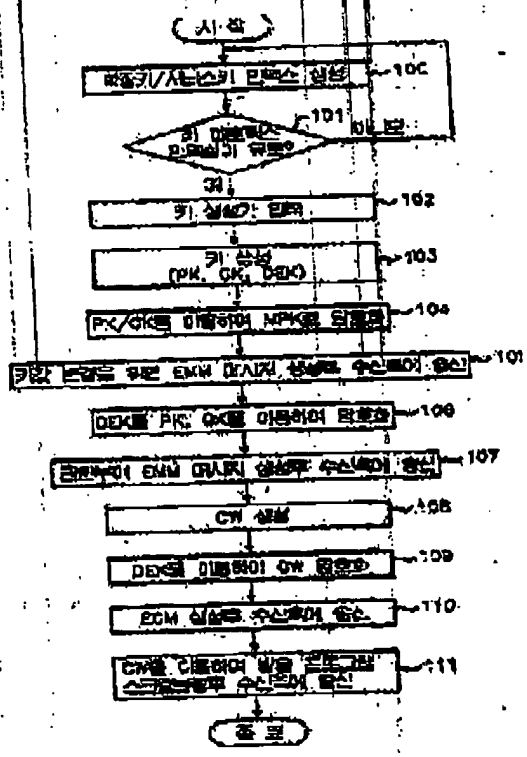
※ 참고사항 : 최초출원 내용에 의하여 공개하는 것임.

도면

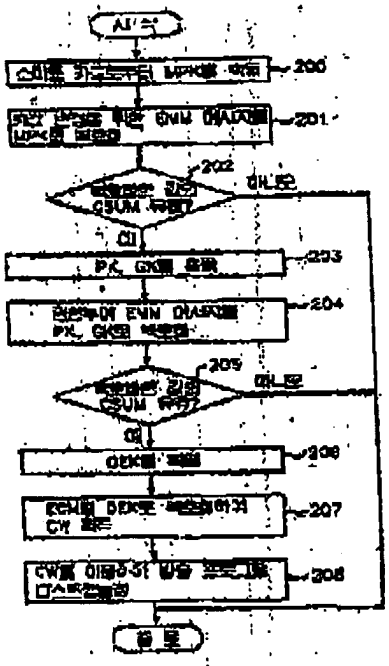


도면2





도면6



RCA 89131 (KR19970064233)

An official report on open to the public patented invention

Open patent invention 1997-0064233

(19) The Republic of Korea Intellectual Property Office (KR)
An official report on open to the public patent invention (A)
(11) Open number 1997-0064233
(43) Open date: September 12, 1997

(21) Application number 1996-0003723
(22) The date of application February 15, 1996

(71) The applicant for a patent the Republic of Korea electronics and communication research worker Yang Seung Thaek
Mega polis city of Taejon, Yoo-Song-ku, Ka-Jeong-dong 161 (zip code: 305-350)

(72) The inventor Kim Shin Hyo
Mega polis city of Taejon, Sogu Sam-Chon-dong, Sang-Rok-su apartment, 103-708
Eun Song Kyong
Mega polis city of Taejon, Yoo-Song-ku, Ka-Jeong-dong 236-1
Cho Jin Man
Mega polis city of Taejon, Sogu Wol-Phyong-dong Jeon-Won apartment, 101-805
Lee Jang Won
Mega polis city of Taejon, Yoo-Seong-ku, Chon-Min-dong Narae apartment 108-502
Cho Hyen Sook
Mega polis city of Taejon, Yoo-Seong-ku, O-Eun-dong, Han-Bit apartment, 131-1306
Kim Dong Kyu
Kyongi-do, Seong-Nam-si, Pun-dang-ku, Soo-Nae-dong, Daelim apartment 102-1301

(74) Agent Park Hae Chon
Yeum Choo Seok

Request for an examination: done

---

(54) The method of processing the message for conditioning (conditionally) limited reception service

---

Summary

The above mentioned invention deals with the processing method for realization of conditioning (conditionally) limited reception service in order to provide limited reception service needed for a fee-charging broadcasting thereof before being transmitted from the transmitting device (1) both eligibility management message (EMM) and eligibility control message (ECM) are encoded and then transmitted, and the receiving device (2) through the process of decryption of the split information only among the approved users encodes it for the second time, and by changing constantly the key value it is possible to maintain the stability of key value and to prevent hacker attacks or faulty subscribers` unlawful access.

Representative table

Table 1

The detailed statement
[The name of the invention]

The method of processing the message for conditioning (conditionally) limited reception service

[A brief explanation of the drawing]

The first table is the system schematic diagram of the above mentioned invention.
The second table deals with based on the above mentioned invention key degree of generation caused by the matrix mode

The sixth table deals with based on the above mentioned invention flow chart of message processing for conditioning (conditional) limited reception service
As far as the above mentioned contents is an essential part open to the public, we did not record technical contents

(57) The sphere of application

Application 1

In order to give to individual subscriber title, for the method of dealing with the message applied to the limited reception system for the conditioning (conditional) limited reception service, which is equipped with the transmission device (1), which includes EMM/ECM generation part (3), which, encoding EMM (Entitlement Management Message), the control word (CW) needed for scramble, the control word (CW), generating the entitlement control message (ECM), which is eligibility message, outputs it, transmission part (4), which, using control word input on the above mentioned EMM/ECM generation part (3), makes the scrambles the broadcasting program, and after multiplexing it along with EMM/ECM information, transmits it via transmission medium, as well as the reception device (2), which has demultiplexing part (5), which, demultiplexing the data, received through the transmission medium, outputs it, processor (6), which, in case of receiving a data, after outputting and demultiplexing the control signal to the above mentioned demultiplexing part (5), outputs EMM/ECM information, using the control word (CW), descrambles received scrambled data and outputs it, smart card (7), which decrypts the split in the EMM, which is input to the above mentioned processor (6), and using again this split key, extracting the session key and control word (CW) from the ECM, outputs it to the above mentioned processor (6), it is referred as the first step (from 100 to 103), when, during creation of the extension key/ service key index, in case index extent is appropriate, personal key (PK), group key (GK), direct authority key (DEK) are created; the second step (104, 105), which, using the personal key (PK), which was created on the above mentioned first step (from 100 to 103), and group key (GK), encodes it into master personal key (MPK), and after creating the EMM message needed for modification of key value, transmits it to the reception side; the third step (106, 107), which, using the personal key (PK) and group key (GK), encodes the direct authority key (DEK), which was created on the first

stage (from 100 to 103), after creation of EMM message, endowing the right, transmits it to the reception side; as well as the fourth step (from 108 to 111), which, after creating the control word (CW), using the direct authority key (DEK), encoding the control word (CW), creates the eligibility control message (ECM), and using the control word (CW), after scrambling the broadcast program, transmits it to the reception side; the fifth step (from 200 to 202), which, using the transmission process, which includes the fourth step, and master personal key (MPK), obtained from the smart card, decrypting the EMM message for alteration of the received key value, estimates whether the check SUM (CSUM), prior to encoding of decrypted data is valid; the sixth step (from 203 to 205), which, in case, if in the above mentioned fifth step (from 200 to 202) it is valid, obtains personal key (PK), group key (GK), decrypting personal key (PK), which obtained EMM message, endowing whether the right of receiving is given or not, into group key (GK), estimates whether the check SUM (CSUM) of the decrypted data is valid; and the seventh step (from 206 to 208), which, in case, it is valid in the above mentioned sixth step (from 203 to 205), obtains the direct eligibility key (DEK), using the obtained direct eligibility key (DEK), decrypting received ECM message, obtains the control word (CW), and using the above mentioned control word (CW), descrambles and outputs the broadcasting program; thus, the method of processing the message for conditioning (conditional) limited reception service has the specific feature, being arranged as a receiving process, which includes seven steps.

Application 2

the application 1 deals with the method of processing the message for conditioning (conditional) limited reception service, where the specific feature is that the data, which is input to key generator in the above mentioned first step (from 100 to 103), consists of the extension key, which is composed of eight bytes from the extension key index value, and service key, which is composed of eight bytes from service key index value.

Application 3

the application 1 deals with the method of processing the message for conditioning (conditional) limited reception service, where the specific feature is that the structure of the EMM message for the endowment of right, is composed of the control field (CTRL), which is composed of the field (Sequence), indicating the sequence number of the message, field (Append), which indicates whether the next message exists or not, field (Encrypt), which indicates the state of using odd or even key during the encoding, as well as field (N), indicating the quantity of vectors, as well as field (KID), indicating the key number, used in vector encoding, as well as the multitude of the encoded vector field (Vector), which are composed of CSUM, which indicates check sum (Checksum) prior to the encoding, and Expiry/KGM, which shows channel number (ID), odd service key address (OSK), even service key address (ESK), odd extension key address (ODN), even extension key address (EDN), eligibility expiration period, and indicates key generation matrix number

Application 4

the application 1 deals with the method of processing the message for conditioning (conditional) limited reception service, where the specific feature is that the structure of message of the EMM for the alteration of the above mentioned key value consists of control field (CTRL), which is composed of field (Sequence), indicating the sequence number of messages, field (Append), indicating whether the next message exists or not, field (Encrypt), which indicates the state of using odd or even key during the encoding, as well as field (N), indicating the quantity of vectors, as well as field (KID), indicating the key number, used in vector encoding, as well as the multitude of the encoded vector fields (Vector), which are composed of CSUM, which indicates the KID, indicating the number of the key, which will alter, GADDR, indicating group address, in case it will be a group key, odd service key address (OSK), even service key address (ESK), odd extension key address (ODN), even extension key address (EDN), CSUM, which indicates check sum (Checksum) prior to the encoding.

Application 5

the application 1 deals with method of processing the message for conditioning (conditional) limited reception service, where the specific feature is that the structure of the above mentioned eligibility control message (ECM) consists of control field (CTRL), which is composed of field (Sequence), indicating the sequence number of messages, field (Append), indicating whether the next message exists or not, field (Encrypt), which indicates the state of using odd or even key during the encoding, as well as field (N), indicating the quantity of vectors, as well as multiple vector field (Vector)

Application 6

the application 5 deals with method of processing the message for conditioning (conditional) limited reception service, where the specific feature is that the above mentioned vector field (Vector) consists of channel number (CH_ID), channel control field (CHctrl), odd control word (OCW), even control word (ECW), a second module of the EPOCH time (time), as well as the configuration of channel (access), present system time (month), and also field, which includes check sum (checksum) (csum) prior to encoding

Application 7

The specific feature of the processing method of message for conditioning (conditional) limited reception service is that the above mentioned OCW, ECW, time/ access/ month/ csum is the encoded information
* Reference information: the above information is opened to the public according to the contents of the most recent application